IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C A. No. 04-1199 (SLR) **PUBLIC VERSION**

DECLARATION OF DR. GEORGE KESIDIS IN SUPPORT OF SRI INTERNATIONAL, INC.'S RESPONSES TO:

(1) DEFENDANTS' JOINT MOTION TO LIMIT THE TESTIMONY OF EXPERT, DR. GEORGE KESIDIS, UNDER FEDERAL RULE OF EVIDENCE 702;

(2) DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY UNDER 35 U.S.C. §§ 102 AND 103;

(3) SYMANTEC'S MOTION FOR SUMMARY JUDGMENT OF NONINFRINGEMENT; AND

(4) ISS'S MOTION FOR SUMMARY JUDGMENT THAT THE ASSERTED CLAIMS OF THE SRI PATENTS-IN-SUIT ARE NOT INFRINGED OR, IN THE ALTERNATIVE, ARE INVALID

I, George Kesidis, declare as follows:

1. I am employed by the Pennsylvania State University. My work address is CSE Dept., 338J IST Building, University Park, PA, 16802, USA. I have also been retained by SRI to render expert opinions and testimony in this matter. I have personal knowledge of the matters stated in this declaration and would testify truthfully to them if called upon to do so.

Expert Qualifications and Knowledge of the Relevant Art

2. I earned a bachelor's degree in electrical engineering in 1988, a master's degree in electrical engineering and computer science ("EECS") in 1990, and a doctorate in EECS from the University of California at Berkeley in 1992.

3. I have conducted continuous research into communications and computer networking since beginning my graduate studies at Berkeley in 1990.

4. I am employed as a tenured Associate Professor (and will become a full Professor on July 1, 2006) in the Electrical Engineering and Computer Science & Engineering Departments of the Pennsylvania State University.

5. Since receiving my Ph.D. in 1992, I have taught courses and written articles on network traffic engineering including traffic modeling, statistical analysis, packet scheduling, and router control methods.

6. Between 1992 and the present date, I obtained numerous grants and consulting contracts in the field of network traffic engineering, a sibling field of cyber security. A significant portion of my research was in the sector of network traffic measurements and associated statistics, an area of overlap between the network traffic engineering and cyber security fields.

7. I began conducting research in the specific field of cyber security in 2000 and by 2001 my collaborators and I had drafted research proposals and papers for submission in this field.

8. When I first entered the cyber security field, I spent several months during the summer and fall of 2000 surveying the literature in order to familiarize myself with earlier work. I also attended security-related talks at several conferences. My review focused mostly on articles and conference proceedings from the previous two years. The review was initially a broad survey of the cyber security field, but I then focused more specifically on areas such as attribution and traceback – research having to do with identifying the source of a suspected attack – and thus read more extensively and further

back in time on those and closely-related subjects. I specifically recall reviewing articles about GrIDS in particular during that timeframe.

9. In 2002, I was awarded a $53,000 grant by Cisco Systems to explore how rapid traceback could be used to improve defenses against diffuse worm and more focused Distributed Denial of Service (DDoS) attacks.

10. In 2003, I began working on a high-profile, multiple-university project on the testing of cyber security defenses. This project, known as EMIST – together with its sister testbed project, DETER – has so far received $11 million in funding from the Department of Homeland Security and the National Science Foundation.

11. In addition to co-investigators of EMIST/DETER (including Philip Porras, one of the named inventors on the patents-in-suit, Felix Wu, and Karl Levitt), I have consulted with numerous other individuals widely known for their expertise in cyber security at conferences and NSF panels in an effort to ascertain the critical problems in the field, previous approaches proposed to address them, and currently promising directions within the field.

12. I have written two books, published more than twenty-five journal articles, and authored over 50 conference papers in the network traffic engineering field, more than one-quarter of which fall specifically within the cyber security discipline.

13. I have also been invited to present more than a dozen talks about this research, including at an internal Cisco Systems security summit, at the Department of Homeland Security, and at universities across North America. In June 2005, I delivered a lecture on the testing of Internet security systems in Tokyo at the 2nd U.S.-Japan Experts Workshop on Critical Information Infrastructure Protection.

14. In addition, I serve as a technical program committee co-chair of the Institute of Electrical and Electronics Engineers ("IEEE") INFOCOM 2007, a major comprehensive networking conference. I have held similar positions at numerous other IEEE conferences, including those that are specific to cyber security (like IEEE

NPSec'05 and ACM SIGCOMM LSAD'06), and I currently serve as a senior member of the IEEE.

15. Based on my review of the literature within that time frame, both at the time I entered the field and over the time I have been actively conducting research, I believe there was no material change in the level of ordinary skill in the field of cyber security between 1998 and 2000-2001. A person of this ordinary level of skill would possess either a bachelor's degree in Computer Science, Electrical Engineering, or Computer Engineering and 5-7 years experience in enterprise-deployed cyber security (or a master's degree in CS, EE, or CE and 3-5 years experience in same). Such a person would also be familiar with the basic, existing techniques of cyber security and their performance and limitations, as well as deployment and maintenance issues of cyber security products.

The Patents-in-suit and "Statistical Detection Methods"

16. I understand that Defendants have asserted that I "admitted" that use of fixed thresholds as part of an intrusion detection analysis always constitutes a "signature-based" method. My deposition testimony, wherein I acknowledge that generating a report of suspicious activity based on a fixed threshold count of failed login attempts can be characterized as a "signature" is in no way an "admission" that *any use* of a fixed threshold is a "signature," and therefore not "statistical" analysis. A threshold can certainly be used as part of a statistical detection algorithm. For example, the threshold itself could be statistically derived. One way of providing such a threshold would be to base it on a moving average over time. On the other hand, the quantity being compared to a threshold, fixed or otherwise, could itself be statistically derived, for example, deriving the ratio of the average number of SYN requests to SYN_ACKs in some statistically significant set of packet data. The use of a "threshold" alone is simply not determinative of whether a detection method is or is not statistical in nature.

17. A type of rudimentary threshold analysis can be used to detect suspicious activity in the context of certain innately suspicious events. For example, a failed login attempt as to a certain type of user account is inherently suspicious. And whereas a single failed login may be ignored as accidental, a sequence, of say, three failed logins is commonly understood by those of skill in the art to be sufficiently suspicious, in and of itself, to require further action. Comparing a count of failed login attempts to a threshold level is considered signature-based detection because it involves *a priori* knowledge of known suspicious activity. In fact, all of the examples given in the patent as lending themselves to "rudimentary, inexpensive signature analysis"—fingers, pings, or failed login requests to accounts such as guest, demo, visitor, anonymous FTP, or employees who have departed the company [Ex. A at 7:50-54][1]—are events that, as individual occurrences, would be considered innately suspicious by a security professional. As such, a very simple threshold count can be used to determine if further action is warranted when dealing with such unique events.

18. Statistical detection methods, as taught by the patents, become necessary when detection is based on "events", in this case individual network packets, that are in and of themselves benign and inherently non-suspicious. For example, individual SYN requests and SYN ACKs are inherently benign. However, an inordinate, unusual spike in the number of unacknowledged SYN requests would be considered suspicious. Detecting SYN Flood attacks requires that the detection engine infer suspicious activity by analyzing aggregate statistics, such as the ratio of SYN Requests to SYN ACKs over time or an accumulated number of packets. Such an analysis is a statistical detection method because it is only by analysis of the statistically significant aggregate of activity that its suspicious nature may be inferred.

19. Alerting on failed login attempts is an example that uses a non-statistical threshold comparison. Discussion of such a method has nothing to do with statistical

[1] All exhibits are attached to this declaration.

analysis, such as the detecting of SYN floods in Symantec's accused products. Failed login attempts are inherently suspicious, and the patent specification lists failed login attempts as one a of a number of specific event types that give rise to suspicion merely by occurring more than a threshold number of times. [*See* Ex. B at 7:52-63]. Also, the specification suggests a different algorithm for detecting failed logins than for detecting SYN Floods because the preferred embodiment uses the signature engine 24 to detect suspicious activity based on failed log-in attempts, but uses profile engine 22, applying statistical methods, to detect SYN Floods.

20. I have read Dr. Hansen's report on non-infringement by the Symantec products. [Ex. C]. Having read Dr. Hansen's report, I am still of the opinion, exactly as stated in my opening report on infringement, that Symantec's accused products perform statistical detection methods as claimed in the claims of the '212 patent and in claim 7 of the '615 patent. I am also still of the opinion that the **REDACTED** compare long-term and short-term statistical profiles as claimed in the '338 patent.

REDACTED

REDACTED

Response to new assertions in ISS's Motion Regarding Non-Infringement

24. I have reviewed ISS's Motion for Summary Judgment that the Asserted Claims of the SRI Patents-in-suit are not Infringed or, in the Alternative, are Invalid and the Declarations in Support Thereof.

REDACTED

Displaying events at a user interface console is not "integration" as that term is used in the claims of the patents-in-suit.

25.

REDACTED

The Disclosure of the "Ji-Nao" Prior Art

27. I understand that the Defendants assert that Ji-Nao anticipates the hierarchical claims of the '203, '615, and '212 patents. The Defendants base this assertion on Fig. 1 of the *Ji-Nao Report*, SYM_P_0070549, and text from that Report ,

SYM_P_0070577]. But the Ji-Nao project did not attempt to achieve hierarchical correlation. The *Ji-Nao Report* proposes that the disclosed system, which performs detection/analysis functions in a local subsystem, could be "extended to a global level and correlate intrusion events among several routers," [Ex. G at SYM_P_0070548], but acknowledges that such extension "is not within the scope of this project." *Id.* Although hierarchical correlation was a goal of the Ji-Nao researchers, as I have discussed in my Rebuttal Report on Validity, Frank Jou, the principal investigator of the Ji-Nao project, testified that the Ji-Nao system did not attain that goal. [*See* Ex. J at ¶ 104, Ex. H at 172:1-173:11, 170:18-171:2]. Ji-Nao does not anticipate the hierarchical claims of the patents in suit because it does not perform hierarchical correlation.

28. I understand further that the Defendants have characterized my statements that Ji-Nao "reacted to network packets" as conceding that Ji-Nao receives packets, and thus anticipates the claims of the '338 patent. The '338 patent discloses and claims receiving network packets and building profiles from measures of the network packets. As stated in my Rebuttal Report on Validity, the Ji-Nao intrusion analysis function does not directly receive network traffic data (i.e., network packets). [Ex. J at ¶ 101]. Instead, Ji-Nao analyzes logs of data generated by network routers. [*Id.*]. Some of the router audit logs reflect the impact of certain types of data packets on the router that received them. [*Id.* at ¶ 102]. Ji-Nao does not receive or analyze the data packets themselves, and therefore cannot build profiles from measures of the network packets. Instead, Ji-Nao builds profiles from measures of audit log data. This is clearly stated in the Ji-Nao Report's discussion of measures: "[w]e would classify the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. . . . These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal." [Ex. G at

SYM_P_0070564]. My statement that Ji-Nao "reacted to network packets" was not a concession that Ji-Nao receives network packets and builds profiles from measures of those packets. Consistent with the Ji-Nao Report and my prior testimony, Ji-Nao "reacts" to network packets only in the sense that it analyzes audit logs that, among other things, represent the impact on routers of certain network packets received by those routers, and builds profiles from measures of those audit logs. Because Ji-Nao does not, however, base its intrusion detection analysis on or build profiles from measures of packets, it does not disclose every limitation of the claims of the '338 patent. Accordingly, Ji-Nao does not anticipate the '338 patent.

I declare under penalty of perjury that the foregoing is true and accurate. Executed this 30th day of June, 2006, in University Park, Pennsylvania.

George Kesidis

CERTIFICATE OF SERVICE

I hereby certify that on July 10, 2006, I electronically filed the **REDACTED – DECLARATION OF DR. GEORGE KESIDIS IN SUPPORT OF SRI INTERNATIONAL, INC.'S RESPONSES TO: (1) DEFENDANTS' JOINT MOTION TO LIMIT THE TESTIMONY OF EXPERT, DR. GEORGE KESIDIS, UNDER FEDERAL RULE OF EVIDENCE 702; (2) DEFENDANTS' JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY UNDER 35 U.S.C. §§ 102 AND 103; (3) SYMANTEC'S MOTION FOR SUMMARY JUDGMENT OF NON-INFRINGEMENT; AND (4) ISS'S MOTION FOR SUMMARY JUDGMENT THAT THE ASSERTED CLAIMS OF THE SRI PATENTS-IN-SUIT ARE NOT INFRINGED OR, IN THE ALTERNATIVE, ARE INVALID** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz Potter Anderson & Corroon LLP Hercules Plaza 1313 North Market Street, 6th Floor P.O. Box 951 Wilmington, DE 19899	Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation
Richard K. Herrmann Morris James Hitchens & Williams PNC Bank Center 222 Delaware Avenue, 10th Floor P.O. Box 2306 Wilmington, DE 19899-2306	Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath